CAPÍTULO 12 A Segurança e os Desafios Éticos da Tecnologia da Informação

VISÃO GERAL DO CAPÍTULO

O objetivo deste capítulo é discutir os controles necessários para o desempenho e segurança dos sistemas de informação, bem como as implicações éticas e impactos sociais da tecnologia da informação.

Seção I: Questões de Segurança e Controle em Sistemas de Informação

1) Discute como se pode promover a qualidade e segurança dos sistemas de informação por uma diversidade de controles , procedimentos e instalações.

Seção II: Desafios Éticos e Sociais da Tecnologia da Informação

1) Discute conceitos éticos fundamentais e como a TI afeta a sociedade no emprego, individualidade, condições de trabalho, privacidade, crime, saúde e soluções para problemas sociais.

OBJETIVOS DO CAPÍTULO

Objetivos do Capítulo

Identificar diversos tipos de controles de sistemas de informação, controles de procedimentos e controles de instalações e explicar como eles podem ser utilizados para garantir a qualidade e segurança dos sistemas de informação.

Discutir maneiras de controlar o desempenho e segurança do uso da Internet pelas empresas e seus usuários finais e parceiros comerciais.

Identificar diversas questões éticas no modo como a tecnologia da informação afeta o emprego, individualidade, condições de trabalho, privacidade, crime, saúde e soluções para problemas sociais.

Propor diversas maneiras pelas quais os usuários finais gerenciais podem ajudar a atenuar os efeitos nocivos e aumentar os efeitos benéficos da tecnologia da informação.

TÓPICOS FUNDAMENTAIS DO CAPÍTULO

Título da Seção

12-1 Por que os Controles São Necessários
12-2 Controles dos Sistemas de Informação
12-3 Controles de Instalações
12-4 Controles de Procedimentos
12-5 Auditoria de Sistemas de Informação
12-6 A Dimensão Ética
12-7 Dimensões Éticas e Sociais da TI
12-8 Questões de Privacidade
12-9 Crimes com o uso do computador
12-10 Questões de Saúde
12-11 Soluções Sociais
12-12 Você e a Responsabilidade Ética

SUGESTÕES DE ENSINO

Deve-se enfatizar a necessidade de controles para os sistemas de informação. A **Figura 12.2** pode servir para fornecer uma visão geral dos diversos tipos de controles necessários para a segurança do sistema de informação. A figura enfatiza que tipos específicos de controles podem ser agrupados em três categorias principais: controles de sistemas de informação, procedimentos e instalações. Novas estimativas de erros de computador e crimes relacionados ao computador poderiam ser utilizadas para convencer os alunos da importância deste tópico. A **Figura 12.3** oferece exemplos de controles de sistemas de informação.

Enfatize para os alunos que esses controles destinam-se a monitorar e manter a qualidade e segurança das atividades de entrada, processamento, saída e armazenamento de um sistema de informação. Exemplos de controles de procedimentos e instalações físicas devem também ser discutidos, principalmente a importância do planejamento de recuperação de desastres. Vários outros slides foram projetados no material do PowerPoint para completar o material no restante da Seção 1.

A **Figura 12.13** resume os principais aspectos das dimensões éticas e sociais da TI. Deve-se enfatizar para os alunos que a TI pode produzir tanto efeitos positivos como negativos na sociedade. Os professores devem passar um tempo discutindo os diferentes tipos de crimes informatizados e por que eles são considerados crimes. A **Figura 12.20** discute fatores ergonômicos a serem considerados no local de trabalho.

NOTAS DE AULA

SEÇÃO I: *Questões de Segurança e Controle em Sistemas de Informação*

12.1 Por que os Controles São Necessários

Os controles são necessários para garantir a qualidade e segurança dos recursos de hardware, software, redes e dados dos sistemas de informação. Os computadores provaram que podem processar grandes volumes de dados e executar cálculos complexos de modo mais preciso do que os sistemas manuais ou mecânicos. Entretanto, sabe-se também que:

- Ocorrem erros em sistemas computadorizados .
- Os computadores têm sido utilizados para fins fraudulentos.
- Os sistemas de computador e seus recursos de software e dados têm sido destruídos acidental ou deliberadamente.

Analisando a BuyDirect e Outras Empresas

Podemos aprender muito a partir deste caso sobre a ameaça de fraude em cartões de crédito e as medidas defensivas que uma empresa pode tomar em transações de comércio eletrônico. Aproveite alguns minutos para ler o caso e iremos discuti-lo (Veja BuyDirect e Outras Empresas na Seção XI).

***Por que os Controles são Necessários:* [Figura 12.2]**

Os controles eficazes fornecem ***segurança dos sistemas de informação***, ou seja:

- A precisão, integridade e segurança das atividades e recursos dos sistemas de informação. Os controles podem minimizar erros, fraude e destruição nos sistemas de informação interconectados que hoje ligam entre si usuários finais e organizações.
- Fornecem ***garantia de qualidade*** para os sistemas de informação. Ou seja, eles podem deixar um sistema de informação computadorizado mais livre de erros e fraude e capaz de fornecer produtos de informação de qualidade mais alta do que os tipos manuais de processamento da informação.
- Reduzem o impacto negativo potencial (e aumentam o impacto positivo) que a tecnologia da informação pode produzir na sobrevivência e sucesso das empresas e na qualidade de vida na sociedade.

Três tipos principais de controle devem ser desenvolvidos para garantir a qualidade e segurança dos sistemas de informação. Essas categorias de controle incluem:

- Controles de sistemas de informação.
- Controles de procedimentos.
- Controles de instalações.

12.2 Controles dos Sistemas de Informação: [Figura 12.3]

Os ***controles dos sistemas de informação*** são métodos e dispositivos que procuram garantir a precisão, validade e propriedade das atividades dos sistemas de informação. Os controles devem ser desenvolvidos para garantir a forma correta de:

- Entrada de dados
- Técnicas de processamento
- Métodos de armazenamento
- Saída de informações

Os controles dos sistemas de informação são projetados para monitorar e manter a qualidade e segurança das atividades de entrada, processamento, saída e armazenamento de um sistema de informação.

Controles de Entrada

A expressão GIGO (*garbage in, garbage out*, ou “entra lixo, sai lixo”) explica a necessidade de controles de entrada. Esses controles incluem:

Senhas e outros códigos de segurança

Telas formatadas para entrada de dados

Sinais audíveis de erro

Máscaras para as teclas de dispositivos de entrada acionados por teclas

Formulários pré-gravados e pré-numerados.

Sistemas de tempo real que podem registrar todas as entradas no sistema em registros de controle em fita magnética que preservam evidência de todas as entradas no sistema. Isto pode incluir a realização de “checagens de razoabilidade” para determinar se os dados introduzidos excedem certos limites especificados ou estão fora de ordem. Isto inclui o cálculo e monitoração de ***totais de controle*** (contagem de registros, totais de lotes *[batch totals]* e totais parciais *[hash totals]*).

Controles de Processamento

Uma vez que os dados tenham sido corretamente registrados em um sistema de computador, eles devem ser corretamente processados. Os controles de processamento identificam erros em cálculos aritméticos e operações lógicas. Eles também são utilizados para garantir que os dados não se percam ou fiquem sem processamento. Os controles de processamento podem incluir controles de hardware e controles de software.

Controles de Hardware

Os ***controles de hardware*** são verificações especiais embutidas no hardware para verificar a precisão do processamento do computador. Exemplos de controles de hardware incluem:

- **Circuitos de Detecção de Falhas**

Estes são os circuitos encontrados dentro do computador utilizados para monitorar suas operações – por exemplo, verificações de paridade, verificações pelo eco, verificações de circuitos redundantes, verificações de sinais aritméticos e verificações de sincronização e voltagem da CPU.

- **Componentes Redundantes**

São dispositivos que verificam e promovem a exatidão de atividades de leitura e gravação – por exemplo, múltiplas cabeças de leitura e gravação em unidades de fita e disco magnético.

- **Microprocessadores de Finalidades Especiais e Circuitos Associados**

São dispositivos como chaves que podem ser utilizados para apoiar diagnósticos e manutenção à distância. Estes permitem aos técnicos o diagnóstico e correção de alguns problemas via links de rede com o computador.

Controles de Software

Os ***controles de software*** têm o objetivo de garantir que os dados corretos estão sendo processados. Exemplos de controles de software incluem:

- Rótulos de arquivos internos que permitem que o computador garanta que o arquivo correto de armazenamento está sendo utilizado e que os dados corretos no arquivo foram processados.
- O estabelecimento de *pontos de verificação* durante o processamento de um programa. Os pontos de verificação são pontos intermediários dentro de um programa que está sendo processado, onde os resultados intermediários são gravados em fita ou disco magnético ou listados em uma impressora. Os pontos de verificação minimizam o efeito de erros de processamento e também ajudam a construir uma *trilha de auditoria* [*audit trail*], que

permite que as transações em processamento sejam acompanhadas ao longo de todas as etapas de processamento.

- Pacotes de software de sistemas especializados conhecidos como ***monitores de segurança de sistemas*** são programas que monitoram o uso de um sistema de computador e protegem seus recursos contra uso não autorizado, fraude e destruição.

Controles de Saída

Os ***controles de saída*** são desenvolvidos para garantir que os produtos de informação estejam corretos e completos e estejam disponíveis de maneira oportuna a usuários autorizados. Exemplos de controles de saída são:

- Documentos e relatórios de saída que são freqüentemente registrados, identificados com revisões de rota e visualmente checados pelo pessoal de entrada/saída.
- Totais de controle sobre a saída que normalmente são comparados com os totais de controle gerados durante as etapas de entrada e processamento.
- Listagens de controle que podem ser produzidas fornecendo evidência em papel para toda saída produzida.
- Formulários de saída pré-numerados que podem ser usados para controlar a perda de documentos importantes.
- Listas de distribuição que garantem que apenas os usuários autorizados recebem saída.
- Acesso à saída que pode ser controlado por códigos de segurança que identificam os usuários que podem receber saída e o tipo de saída que eles estão autorizados a receber.
- Usuários finais que recebem saída que devem ser incentivados a fornecer feedback sobre a qualidade da saída.

Controles de Armazenamento

Os recursos de aremazenamento de dados são uma importante consideração. As responsabilidades de controle para arquivos de programas de computador e bancos de dados organizacionais podem envolver:

- Atribuir as responsabilidades de controle a especialistas de centros de dados e administradores de bancos de dados.

- Garantir a proteção contra uso não autorizado ou acidental utilizando programas de segurança que exigem identificação apropriada antes de poderem ser utilizados.
- Utilizar códigos de contas, ***senhas*** e outros ***códigos de segurança*** para permitir acesso apenas a usuários autorizados
- Outros controles de armazenamento que podem utilizar tecnologias de *criptografia* e *cartão inteligente*.
- Estabelecer um catálogo de usuários autorizados para permitir ao sistema de computador identificar usuários qualificados e determinar que tipos de informação eles estão autorizados a receber.
- Ter ***arquivos de reserva***, que são arquivos duplicados que podem ser armazenados em um local distante do centro de computação.
- Proteger arquivos utilizando medidas de *retenção de arquivo* que envolvem cópias de armazenamento de arquivos mestre e arquivos de transações de períodos anteriores.
- Manter diversas gerações de arquivos para fins de controle (arquivos *filho, pai, avô,* etc.).

12.3 Controles de Instalações

Controles de instalações são métodos que protegem as instalações de computação e redes de uma organização e seu conteúdo contra a perda ou destruição. As redes e centros de computação estão sujeitos a casualidades como:

- Acidentes
- Desastres naturais
- Sabotagem
- Vandalismo
- Uso não autorizado
- Espionagem industrial
- Destruição e roubo de recursos

Segurança de Rede

A segurança de uma rede pode ser fornecida por pacotes de software de sistemas especializados conhecidos como ***monitores de segurança de sistemas***. Os monitores de

segurança de sistemas são programas que monitoram o uso de sistemas e redes de computadores e os protegem do uso não autorizado, fraude e destruição. Esses programas fornecem:

- As medidas de segurança necessárias para permitir que apenas usuários autorizados acessem as redes.
- Os monitores de segurança também controlam o uso dos recursos de hardware, software e dados de um sistema de computador.
- Os programas de segurança monitoram o uso de redes de computadores e coletam estatísticas sobre quaisquer tentativas de uso impróprio. Em seguida, produzem relatórios para ajudar na manutenção da segurança da rede.

Criptografia

A ***criptografia*** de dados tornou-se uma maneira importante de proteger dados e outros recursos de rede de computadores, principalmente na Internet, intranets e extranets. Características da criptografia incluem:

- Senhas, mensagens, arquivos e outros dados que podem ser transmitidos de forma embaralhada e desembaralhados pelos sistemas de computadores apenas para usuários autorizados.
- O uso de algoritmos matemáticos especiais, ou *chaves*, para transformar dados digitais em um código embaralhado antes que esses dados sejam transmitidos e para decodificá-los quando forem recebidos.
- O método mais amplamente utilizado de criptografia que utiliza um par de *chaves públicas* e *privadas* exclusivas de cada indivíduo. Um e-mail, por exemplo, poderia ser embaralhado e codificado utilizando uma única chave pública para o destinatário, que é conhecida pelo remetente. Após a transmissão do e-mail, apenas a chave privada secreta do destinatário poderia desembaralhar a mensagem.
- Os programas de criptografia que são vendidos como produtos independentes ou embutidos em outro software utilizado para o processo de criptografia.

Fire Wall

Outro método importante para controle e segurança na Internet e outras redes é o uso de computadores e software. Características de computadores e software fire wall incluem:

- Um fire wall de rede é um sistema de computador "guardião" que protege as intranets e outras redes de computadores de uma empresa contra a invasão, funcionando como um filtro e ponto seguro de transferência para acesso à e da Internet e outras redes.
- Um computador de rede fire wall filtra todo o tráfego de rede em busca de senhas corretas ou outros códigos de segurança e somente permite transmissões autorizadas para dentro e para fora da rede.
- Os fire walls se tornaram um componente essencial de organizações que se conectam com a Internet, em virtude da vulnerabilidade e falta de segurança da Internet.
- Os fire walls podem deter, mas não evitar inteiramente, o acesso não autorizado (*hacking*) às redes de computadores. Em alguns casos, um fire wall pode permitir acesso apenas a partir de locais credenciados na Internet para determinados computadores dentro do fire wall. Ou pode permitir que apenas informações "seguras" sejam transmitidas.
- Em alguns casos, é impossível saber se o uso de um determinado serviço de rede é seguro ou inseguro e, por isso, todos os pedidos devem ser bloqueados. O fire wall pode então fornecer substitutos para alguns serviços de rede que desempenham a maioria das mesmas funções mas que são menos vulneráveis a invasão.

Controles de Proteção Física

Fornecer segurança máxima e proteção contra desastres para os recursos de computação de uma organização exige diversos tipos de controles. O acesso a centros de computação e áreas de trabalho do usuário final, por exemplo, é permitido apenas ao pessoal autorizado por técnicas como:

- Símbolos de identificação
- Fechaduras eletrônicas
- Alarmes contra roubo
- Polícia de segurança
- Circuito fechado de TV e outros sistemas de detecção

Os centros de computação podem ser protegidos de desastres por salvaguardas como:

- Sistemas de detecção e extinção de incêndio
- Caixas fortes de armazenamento à prova de incêndio para a proteção de arquivos
- Sistemas de energia elétrica de emergência
- Escudos eletromagnéticos
- Controles de temperatura, umidade e poeira.

Controles Biométricos

Os ***controles biométricos*** são medidas de segurança fornecidas por dispositivos de computador que medem características físicas que tornam cada indivíduo único. Isto inclui:

- Verificação de voz
- Análise de digitação
- Impressões digitais
- Escaneamento de retina
- Geometria de mão
- Reconhecimento facial
- Dinâmica de assinatura
- Análise de padrões genéticos

Controles de Falhas no Computador

Uma série de controles é necessária para evitar falhas de computador ou minimizar seus efeitos. Os de computadores podem falhar em virtude de:

- Queda de energia
- Defeitos nos circuitos eletrônicos
- Problemas na rede de telecomunicações
- Erros de programação ocultos
- Erros do operador do computador
- Vandalismo eletrônico

O departamento de serviços de informação normalmente toma medidas para evitar a falha no equipamento e minimizar seus efeitos prejudiciais. Por exemplo:

- Programas de manutenção preventiva de hardware e administração de atualizações de software são comuns.
- Utilizar computadores dotados de capacidades de manutenção automática e à distância.
- Estabelecer padrões para fornecimento de energia elétrica, ar condicionado, controle de umidade e padrões de prevenção de incêndio
- Obter uma capacidade de backup de um sistema de computador com organizações de recuperação de desastres.
- Programar e implementar principais mudanças de hardware ou software para evitar problemas.
- Treinamento e supervisão de operadores de computadores.
- Utilizar sistemas de computação ***tolerantes a falhas*** (capacidades à *prova de falhas* e *tolerante a falhas*)

Tolerância a Falhas

Esses sistemas evitam a falha do computador utilizando múltiplas CPUs, periféricos e software de sistemas.

- ***À Prova de Falhas***

À prova de falhas se refere a sistemas de computador que continuam a operar no mesmo nível de desempenho depois de uma falha maior.

- ***Tolerante a Falhas***

Tolerante a falhas se refere a sistemas de computador que continuam a operar em um nível reduzido, porém aceitável, depois de uma falha do sistema.

12.4 Controles de Procedimentos

Controles de procedimentos são métodos que especificam como os recursos de computadores e redes de uma organização devem ser operados para a segurança máxima. Eles facilitam a

precisão e integridade das operações dos computadores e das atividades de desenvolvimento de sistemas. Isto inclui:

- Padrões de procedimento e documentação
- Requisitos de Autorização
- Recuperação de Desastres
- Controles para a Computação pelo Usuário Final

Procedimentos-padrão

Normalmente, uma organização de SI desenvolve e adota procedimentos padrão para a operação de sistemas de informação. Os procedimentos padrão promovem a qualidade e minimizam as chances de erros e fraude. Eles ajudam usuários finais e especialistas de SI a saberem o que se espera deles em termos de procedimentos operacionais e qualidade de sistemas. Além disso, a documentação do projeto de software e dos sistemas e a operação do sistema devem ser desenvolvidas e mantidas atualizadas. A documentação também é inestimável na manutenção de um sistema à medida que são feitos os melhoramentos necessários.

Requisitos de Autorização

Os pedidos de desenvolvimento de sistemas, alterações de programas ou processamento de computação normalmente são submetidos a uma revisão formal pela administração antes de ser dada a autorização. A autorização minimiza os efeitos prejudiciais sobre a precisão e integridade das operações em curso de sistemas e redes.

Recuperação de Desastres

Furacões, terremotos, incêndios, enchentes, atos terroristas e criminosos e falha humana podem danificar seriamente os recursos de computação de uma organização. Muitas organizações como companhias aéreas e bancos, por exemplo, são incapacitadas até pela perda de algumas horas de poder de computação. É por isso que é importante que as organizações desenvolvam procedimentos de ***recuperação de desastres*** e os formalizem em um *plano de recuperação de desastres*. Esse plano especifica quais funcionários participarão na recuperação do desastre e quais serão suas obrigações; que hardware, software e

instalações serão utilizados e a prioridade das aplicações que serão processadas. Acordos com outras empresas para o uso de instalações alternativas como local de recuperação de desastres e armazenamento externo dos bancos de dados de uma organização também fazem parte de um esforço eficaz de recuperação de desastres.

Controles para a Computação pelo Usuário Final

Muitas aplicações desenvolvidas pelo usuário final estão desempenhando funções organizacionais extremamente importantes que são decisivas para o sucesso e sobrevivência da empresa. Elas podem muitas vezes ser chamadas de aplicações do usuário final *críticas à empresa*. Os controles envolvidos nas aplicações dos usuários finais devem ser os mesmos que aqueles que constituem prática padrão no desenvolvimento de aplicações por departamentos de profissionais de SI.

12.5 Auditoria de Sistemas de Informação

Um departamento de serviços de informação deve ser periodicamente examinado pelo pessoal de auditoria interna da empresa. Além disso, auditorias periódicas realizadas por auditores externos de firmas de contabilidade profissional constituem uma boa prática de negócios. Tais auditorias devem revisar e avaliar se foram desenvolvidos e implementados controles corretos e adequados dos sistemas de informação, controles de procedimento, controles de instalações e outros controles administrativos. Existem duas abordagens básicas para ***auditoria de sistemas de informação*** – ou seja, a realização de auditoria das atividades de processamento de informações dos sistemas de informação computadorizados. Essas abordagens são conhecidas como:

- Auditoria em torno do computador
- Auditoria por meio do computador

Auditoria em torno do computador

A auditoria em torno do computador envolve a verificação da precisão e propriedade de entrada e saída do computador produzida sem avaliação do software que processou os dados.

Vantagens deste método:

- Método simples e fácil que não exige auditores com experiência em programação.

Desvantagens deste método:

- Não acompanha uma transação ao longo de todas as suas etapas de processamento
- Não testa a precisão e integridade do software utilizado.

Auditoria por meio do computador

A *auditoria por meio do computador* envolve a verificação da precisão e integridade do software que processa os dados, bem como da entrada de dados e saída produzidos pelos sistemas e redes de computadores.

Vantagens deste método:

- Testa a precisão e integridade dos programas de computador.
- Testa a entrada e saída do sistema de computador.

Desvantagens deste método:

- Exige um conhecimento do sistema de computador e operações de rede e desenvolvimento de software.
- Dispendioso para algumas aplicações de computador.

Um dos objetivos importantes desses procedimentos de auditoria é testar a integridade da trilha de auditoria de uma aplicação. Uma **trilha de auditoria** pode ser definida como a presença de documentação que permite que uma transação seja rastreada ao longo de todas as etapas de seu processamento de informações. A trilha de auditoria dos sistemas de informação manuais são bastante visíveis e fáceis de rastrear, entretanto, os sistemas de informação baseados em computador alteraram a forma da trilha de auditoria.

SEÇÃO II: *Desafios Éticos e Sociais da Tecnologia da Informação*

Analisando a Warroom Research e o Sun-Trust Banks

Podemos aprender muito a partir deste caso sobre as questões de segurança das redes e os desafios que cercam o uso da tecnologia da informação nas empresas. Aproveite alguns minutos para ler o caso e iremos discuti-lo (Veja Warroom Research e Sun-Trust na Seção XI).

12.6 A Dimensão Ética

A ***revolução da informação*** com sua tecnologia da informação ampliou drasticamente nossa capacidade para adquirir, manipular, armazenar e comunicar informações. A TI tornou mais fácil se comunicar, trabalhar em cooperação, compartilhar recursos e tomar decisões, tudo eletronicamente. A tecnologia da informação também tornou possível o engajamento eletrônico em práticas empresariais éticas ou antiéticas em qualquer lugar do mundo.

As dimensões éticas de controvérsia que você como gerente pode ter de encarar incluem:

- Você deve monitorar eletronicamente as atividades de trabalho e o correio eletrônico de seus funcionários?
- Você deve deixar os funcionários utilizarem seus computadores de trabalho para atividades particulares ou levarem cópias de softwares para suas casas para uso pessoal?
- Você deve acessar eletronicamente os registros de pessoal ou as estações de trabalho de seus funcionários?
- Você deve vender para outras empresas informações sobre clientes extraídas dos seus sistemas de processamento de transações?

Fundamentos Éticos

Existem diversas ***filosofias éticas*** que você pode utilizar que ajudam a orientá-lo na tomada de decisões éticas.

- Egoísmo
- Lei Natural
- Utilitarismo
- Respeito pelas Pessoas

- ***Egoísmo***

O que é melhor para um determinado indivíduo é o certo.

- ***Lei natural***

Os homens devem promover sua própria saúde e vida, propagar-se, buscar conhecimento do mundo e de Deus, buscar relações íntimas com outras pessoas e submeter-se à autoridade legítima.

- ***Utilitarismo***

São corretas as ações que produzem o bem maior para o maior número de pessoas.

- ***Respeito pelas pessoas***

As pessoas devem ser tratadas como fim e não como meio para um fim; e as ações são corretas se todos adotarem a regra moral pressuposta pela ação.

Existem ***modelos éticos*** de como os seres humanos aplicam sua filosofia ética escolhida às decisões e escolhas que precisam fazer diariamente no trabalho e em outras áreas de sua vida. Uma teoria se concentra nos processos de tomada de decisão das pessoas e enfatiza como os vários fatores ou as nossas percepções desses fatores afetam nosso processo de tomada de decisão ética. Outra, a teoria do estágio comportamental, afirma que as pessoas passam por diversos estágios de evolução moral antes de se fixarem em um nível de raciocínio ético.

Ética Empresarial

A ***ética empresarial*** pode ser subdividida em duas áreas distintas:

- A primeira diz respeito às práticas ilegais, antiéticas e questionáveis de gerentes ou organizações, suas causas e suas possíveis correções.
- A segunda diz respeito às numerosas questões éticas que os gerentes devem enfrentar como parte de suas decisões empresariais cotidianas.

Os gerentes utilizam diversas alternativas importantes quando confrontados com decisões éticas sobre questões de negócios. Essas alternativas incluem:

- **Teoria do Acionista**

Sustenta que os gerentes são agentes dos acionistas e sua única responsabilidade ética é aumentar os lucros da empresa sem violar a lei ou se envolver em práticas fraudulentas.

- **Teoria do Contrato Social**

Afirma que as empresas possuem responsabilidades éticas para com todos os membros da sociedade, o que permite às empresas existirem com base em um contrato social.

- **Teoria das partes interessadas** [*stakeholder theory*]

Sustenta que os gerentes possuem uma responsabilidade ética na administração de uma empresa para o benefício de todo o seu público, que são todos os indivíduos e grupos que possuem um interesse ou um direito em uma empresa.

12.7 Dimensões Éticas e Sociais da TI: [Figura 12.13]

O uso da TI nos negócios possui impactos importantes sobre a sociedade e, com isso, levanta sérias considerações éticas em áreas como:

- Privacidade
- Crime
- Saúde
- Condições de Trabalho
- Individualidade
- Emprego e
- Busca de soluções sociais por meio da TI

Nota: Os alunos devem percebem que a tecnologia da informação pode produzir um efeito benéfico e também um efeito negativo em cada uma das áreas listadas acima.

A TI e o Emprego

O impacto da TI sobre o ***emprego*** é uma preocupação ética importante e está diretamente relacionada ao uso de computadores para alcançar a automação. O uso da TI gerou novos empregos e aumentou a produtividade. Entretanto, ela ainda tem provocado uma redução significativa em alguns tipos de oportunidades de trabalho.

A TI e a Individualidade

Uma crítica freqüente à tecnologia da informação diz respeito ao seu efeito negativo sobre a ***individualidade*** das pessoas. Os sistemas computadorizados são criticados como:

- Sistemas impessoais que desumanizam e despersonalizam as atividades, já que eliminam as relações humanas presentes nos sistemas sem computadores. As pessoas sentem uma perda de identidade.
- Sistemas em que as pessoas sentem uma perda de individualidade já que alguns exigem a arregimentação do indivíduo e exigem adesão estrita a procedimentos detalhados.

Os sistemas baseados em computador podem ser ergonomicamente projetados para acomodar ***fatores humanos*** que:

- Minimizem a despersonalização e a arregimentação.
- Projetem softwares que sejam personalizados *[people-oriented]* e "amigáveis ao usuário".

A TI e Condições de Trabalho

A TI eliminou algumas tarefas monótonas ou perversas no escritório e na fábrica que anteriormente tinham de ser executadas por pessoas. Dessa forma, pode-se dizer que a TI eleva a *qualidade do trabalho*.

Entretanto, muitas operações automatizadas são também criticadas por relegarem as pessoas a um papel de apoio de "não fazer coisa alguma".

Monitoração pelo Computador

Uma das questões éticas mais explosivas concernentes à qualidade do trabalho é a ***monitoração pelo computador***. Os computadores estão sendo utilizados para monitorar a

produtividade e o comportamento de milhões de funcionários em seu trabalho. Segundo se supõe, a monitoração por computador é feita para que os empregadores possam coletar dados de produtividade sobre seus funcionários para aumentar a eficiência e qualidade do serviço. A monitoração por computador tem sido criticada como antiética porque:

- É utilizada para monitorar indivíduos, não apenas o trabalho, e essa monitoração é realizada continuamente, violando assim a privacidade e liberdade pessoal dos trabalhadores.
- É considerada uma invasão da privacidade dos funcionários porque, em muitos casos, eles não sabem que estão sendo monitorados ou não sabem como a informação está sendo utilizada.
- O direito legal do funcionário de mover processo pode ser prejudicado pelo uso impróprio dos dados coletados para tomar decisões pessoais.
- Ela aumenta a tensão sobre os funcionários que devem trabalhar sob constante vigilância eletrônica.
- Ela tem sido responsabilizada por problemas de saúde entre os trabalhadores monitorados.
- Ela tem sido responsabilizada por roubar os trabalhadores da dignidade de seu trabalho.

12.8 Questões de Privacidade

O poder da TI de armazenar e recuperar informações pode ter um efeito negativo no ***direito à privacidade*** de cada indivíduo. Algumas importantes questões de privacidade que estão sendo debatidas nas empresas e no governo incluem as seguintes:

- Acessar trocas de correspondência e registros de computador privativos de indivíduos e coletar e compartilhar informações sobre indivíduos obtidas a partir de suas visitas a sites e grupos de notícias da Internet (violação da privacidade).
- “Saber” sempre onde uma pessoa está, principalmente quando os serviços de telefonia celular e paging se tornam mais estreitamente associados com as pessoas do que com os lugares (monitoração por computador).
- Utilizar informações de clientes para comercializar serviços adicionais (cruzamento de informação por computador).

- Coletar números telefônicos e outras informações pessoais para montar perfis de cada cliente (arquivos pessoais não autorizados).
- Utilizar equipamento automatizado seja para gerar chamadas ou para colher informações do usuário (identificação de chamadas).

Privacidade na Internet

A Internet é famosa por dar a seus usuários uma sensação de anonimato quando, na realidade, eles são altamente visíveis e estão abertos a violações de sua privacidade. Grande parte da Internet e de sua Rede Mundial de Computadores e grupos de notícias ainda constitui uma fronteira eletrônica escancarada e insegura sem quaisquer regras rígidas sobre quais informações são pessoais e privativas.

Privacidade no E-Mail

As empresas possuem diferentes políticas de privacidade, principalmente quando estas se aplicam ao correio eletrônico. Algumas empresas, por exemplo, nunca monitoram as mensagens de e-mail de seus funcionários, ao passo que outras afirmam que se reservam o direito de fazê-lo. Algumas empresas monitoram constantemente e-mails, enquanto outras o fazem apenas se percebem que há uma razão para suspeitar que um funcionário o esteja utilizando para uma atividade ilegal ou não autorizada.

Cotejo de Computadores

O ***cotejo de computadores*** é o uso de computadores para exibir e equiparar dados sobre características pessoais fornecidos por uma diversidade de sistemas de informação baseados em computador e bancos de dados com o objetivo de identificar indivíduos para fins empresariais, governamentais e outros. O uso não autorizado ou equívocos no cotejo de computadores de dados pessoais podem ser uma ameaça à privacidade. O perfil pessoal de um indivíduo, por exemplo, pode ser incorretamente combinado com o de uma outra pessoa.

Legislação sobre Privacidade

Nos Estados Unidos, a Lei Federal de Privacidade regulamenta rigidamente a coleta e uso de dados pessoais por agências governamentais. A lei especifica que os indivíduos têm o direito

de inspecionar seus registros pessoais, fazer cópias e corrigir ou eliminar informações errôneas ou confusas.

A Lei Federal de Privacidade especifica que as agências federais:

- Devem anualmente divulgar os tipos de arquivos de dados pessoais que elas mantêm.
- Não podem revelar informações pessoais sobre um indivíduo a nenhum outro indivíduo ou agência exceto sob certas condições estritas.
- Devem informar os indivíduos sobre as razões para estarem lhes solicitando informações pessoais.
- Devem reter registros de dados pessoais apenas se estes forem “relevantes e necessários para realizar” um propósito legal da agência.
- Devem estabelecer salvaguardas administrativas, técnicas e físicas apropriadas para garantir a segurança e confidencialidade de registros.

O Congresso dos Estados Unidos aprovou a Lei de Privacidade nas Comunicações Eletrônicas e a Lei sobre Fraude e Abuso do Computador em 1986. Essas ***leis de privacidade*** federais são uma das tentativas principais de aplicar a privacidade de arquivos e comunicações baseados em computador. Essas leis proíbem a interceptação de mensagens de comunicações de dados, roubo ou destruição de dados ou invasão dos sistemas de computadores relacionados ao governo federal.

Difamação e Censura por Computador

O lado oposto do debate da privacidade é o direito das pessoas de saberem sobre assuntos que outras podem desejar manter reservados (liberdade de informação), o direito das pessoas de expressarem suas opiniões sobre esses assuntos (liberdade de discurso) e o direito das pessoas de publicarem essas opiniões (liberdade de imprensa). Alguns dos maiores campos de batalha no debate são os *bulletin boards*, caixas de e-mail e arquivos on-line da Internet e redes públicas de informação como a Prodigy, CompuServe e America Online. As armas que estão sendo utilizadas nesta batalha incluem o *flame mail*, leis sobre difamação e censura.

Spamming – é o envio indiscriminado de e-mail não solicitado para muitos usuários da Internet. O spamming é a tática favorita dos remetentes de massas de propagandas não solicitadas ou *junk e-mail*.

Flaming – é a prática de enviar mensagens de e-mail extremamente críticas, detrativas e muitas vezes vulgares (flame mail), ou mensagens por BBSs para outros usuários na Internet ou serviços on-line. O flaming é principalmente dominante em alguns dos BBSs de grupos de discussão de interesses especiais na Internet. A Internet está muito vulnerável a abusos uma vez que perde atualmente o policiamento formal e apresenta falta de segurança.

12.9 Crime com o uso do computador

O crime com o uso do computador é a ameaça causada pelas ações criminosas ou irresponsáveis de usuários de computadores que estão tirando proveito do uso generalizado das redes de computadores em nossa sociedade. Por isso, ele constitui uma ameaça maior ao uso ético da TI. O crime informatizado apresenta sérias ameaças à integridade, segurança e qualidade da maioria dos sistemas de informação das empresas e, com isso, faz do desenvolvimento de métodos eficazes de segurança uma prioridade máxima.

Legislação sobre Crimes com o uso do computador

A Lei sobre Fraude e Abuso de Computadores dos Estados Unidos de 1986 define o crime informatizado como uma das atividades envolvendo acesso a computadores de "interesse federal" (utilizados pelo governo federal) ou operando no comércio interestadual ou exterior:

- Com o intuito de fraudar
- Resultando em uma perda de mais de 1.000 dólares
- Para obter acesso a certos sistemas de computação médica.
- Traficar senhas de acesso a computadores também é proibido.

As penalidades para violações da Lei sobre Fraude e Abuso de Computadores dos Estados Unidos incluem:

- Um a cinco anos de prisão para um primeiro delito

- Dez anos para um segundo delito
- Vinte anos para três ou mais delitos
- As multas podem chegar a 250.000 dólares ou duas vezes o valor dos dados roubados

A Associação dos Profissionais de Tecnologia da Informação (Association of Information Technology Professionals, ou AITP) define o crime informatizado como:

- O uso, acesso, modificação e destruição não autorizados de recursos de hardware, software, dados ou rede.
- A divulgação não autorizada de informações.
- A cópia não autorizada de softwares
- A negação de acesso a um usuário final aos seus próprios recursos de hardware, software, dados ou rede.
- O uso ou conspiração para uso de recursos de computação para obter ilegalmente informações ou propriedade tangível.

Exemplos de Crime com o uso do computador

O crime com o uso do computador envolve atividades criminosas utilizando computadores. Isto normalmente inclui:

- Roubo de dinheiro, serviços, softwares e dados
- Destruição de dados e softwares, principalmente por vírus de computador
- Acesso malicioso ou hacking na Internet ou outras redes de computadores
- Violação da privacidade
- Violação da lei anti-truste ou internacional.

Crime pela Internet

Os hackers conseguem monitorar e-mail, acesso a servidores da Web ou transferências de arquivo para extraírem senhas ou roubarem arquivos da rede ou inserirem dados que podem fazer com que um sistema dê acesso a intrusos. Um hacker também pode utilizar serviços remotos que permitem que um computador em uma rede execute programas em outro computador para obter acesso privilegiado dentro de uma rede. A Telnet, uma ferramenta

para uso interativo de computadores remotos, pode ajudar um hacker a descobrir informações para planejar outros ataques. Os hackers têm utilizado a Telnet para acessar porta de e-mail de um computador, por exemplo, para monitorar mensagens de e-mail em busca de senhas e outras informações sobre contas de usuários e recursos de rede privilegiados.

Roubo de Dinheiro

Muitos crimes com o uso do computador envolvem o roubo de dinheiro. Eles quase sempre envolvem a alteração fraudulenta de arquivos do computador para encobrir os rastros dos ladrões ou para usufruir do dinheiro de outros com base em registros falsificados.

Roubo de Serviços

O uso não autorizado de um sistema de computador é chamado de ***roubo de serviços***. Um exemplo comum é o uso não autorizado de redes de computadores da empresa por funcionários. Isto pode ir da realização de consultas privadas ou finanças pessoais, ou jogo de vídeo games, até o uso não autorizado da Internet pelas redes da empresa. Softwares de monitoração de redes, conhecidos como *sniffers* (farejadores), são freqüentemente utilizados para monitorar o tráfego da rede para avaliar a capacidade da rede, além de revelar evidência de uso impróprio.

Roubo de Software

Programas de computador são propriedade valiosa e por isso estão sujeitos a roubo dos sistemas de computador. A reprodução não autorizada de software, ou ***pirataria de software***, é uma forma importante de roubo de software porque o software é propriedade intelectual protegida por lei de direitos autorais e contratos de licença com o usuário.

Alteração ou Roubo de Dados

Fazer alterações ilegais ou roubar dados é outra forma de crime informatizado.

Acesso Indevido

Hacking é o uso obsessivo de computadores ou o acesso e uso não autorizados de sistemas de computação em rede. Hackers ilegais (também conhecidos como *crackers*) podem roubar ou danificar dados e programas.

Vírus de Computador – Destruição de Dados e Software

Um dos mais destrutivos exemplos de crime informatizado envolve a criação de ***vírus de computador*** ou *vermes de computador*. Esses vírus normalmente entram em um sistema de computação por meio de cópias de software ilegais ou emprestadas ou por meio de links de rede para outros sistemas de computador. Um vírus normalmente copia a si mesmo nos programas do sistema operacional do computador e de lá para o disco rígido e em quaisquer discos flexíveis inseridos. Programas de vacina e programas de prevenção e detecção de vírus são disponíveis, mas podem não funcionar para novos tipos de vírus.

Vírus – é um código de programa que não pode funcionar sem ser inserido em outro programa.
Verme – é um programa distinto que pode rodar sem assistência.

12.10 Questões de Saúde

O uso da TI no local de trabalho levanta uma série de ***questões de saúde***. O uso intenso de computadores é tido como causador de problemas de saúde como:

- Estresse no trabalho
- Lesões em músculos do braço e pescoço
- Tensão ocular
- Exposição a radiação
- Morte por acidentes provocados por computador

Ergonomia: **[Figura 12.20]**

As soluções para alguns problemas de saúde são baseadas na ciência da ***ergonomia***, às vezes chamada de *engenharia de fatores humanos*. A meta da ergonomia é projetar ambientes de

trabalho saudáveis que sejam seguros, confortáveis e agradáveis para as pessoas trabalharem, aumentando assim o moral e a produtividade do funcionário.

A ergonomia enfatiza a concepção saudável do local de trabalho, estações de trabalho, computadores e outras máquinas e até de pacotes de software. Outras questões de saúde podem exigir soluções ergonômicas que enfatizem mais o desenho do cargo do que o desenho do local de trabalho.

12.11 Soluções Sociais

A tecnologia da informação pode produzir muitos efeitos benéficos na sociedade. A TI pode ser utilizada para solucionar problemas humanos e sociais por meio de ***soluções sociais*** como:

- Diagnóstico médico
- Instrução auxiliada por computador
- Planejamento de programas governamentais
- Controle da qualidade ambiental
- Aplicação das leis

12.12 Você e a Responsabilidade Ética

Como usuário final empresarial, você tem a responsabilidade de fazer algo com relação a alguns abusos da tecnologia da informação no local de trabalho. Essas responsabilidades incluem desempenhar adequadamente seu papel como um recurso humano vital nos sistemas de informação baseados em computador que você ajuda a desenvolver e utiliza em suas organizações.

O código da AITP fornece diretrizes para conduta ética no desenvolvimento e uso da tecnologia da informação. Os usuários finais e os profissionais de SI viveriam de acordo com suas responsabilidades éticas se adotassem voluntariamente essas diretrizes. Você pode ser, por exemplo, um ***usuário final responsável***:

- Atuando com integridade
- Melhorando sua competência profissional
- Estabelecendo padrões elevados de desempenho pessoal
- Assumindo responsabilidade por seu trabalho
- Aprimorando a saúde, privacidade e bem-estar geral do público

LINK

Trilha de Auditoria

Exame periódico da precisão e integridade dos sistemas de informação.

Auditoria de Sistemas de Informação

Um departamento de serviços de informação deve ser periodicamente examinado (por auditoria) pelo pessoal de auditoria interna. Além disso, auditorias periódicas realizadas por auditores externos de firmas de contabilidade profissional constituem uma boa prática de negócios.

Arquivos de Reserva

Arquivos de reserva são arquivos de dados ou programas duplicados. Esses arquivos podem ser armazenados fora das instalações, ou seja, em um local distante do centro de computação, às vezes em caixas fortes de armazenamento especial em locais remotos.

Controles Biométricos

Métodos de segurança baseados no computador que medem traços e características físicas tais como impressões digitais, impressões de voz, escaneamento de retina e assim por diante.

Ética Empresarial

Uma área da filosofia ética relacionada ao desenvolvimento de princípios éticos e à promoção de comportamento e práticas éticas na realização de tarefas e tomada de decisões nas empresas.

Crime com o uso do computador

Ações criminosas realizadas por meio dos sistemas de informação, principalmente com o objetivo de fraudar, destruir ou fazer uso não autorizado de recursos de sistemas de computador.

Crime com o uso do computador – Exemplos

Roubo de dinheiro, serviços e informações – incluindo roubo de software, além de crimes envolvidos em alterações e destruição de dados.

Crime com o uso do computador – Leis

Leis anti-crime com o uso do computador estão sendo desenvolvidas para proteger organizações e seus recursos de dados.

Cruzamento de informação por Computador

Utilização de computadores para exibir e equiparar dados sobre características individuais fornecidos por uma diversidade de sistemas de informação baseados em computador e bancos de dados para identificar indivíduos para fins comerciais, governamentais ou outros.

Monitoração pelo Computador

Utilizar computadores para monitorar o comportamento e a produtividade de trabalhadores no serviço e no local de trabalho.

Vírus de Computador

Código de programa que copia suas rotinas destrutivas nos sistemas de computadores de qualquer pessoa que acessa sistemas de computadores que utilizaram o programa ou que utiliza cópias de dados ou programas tirados a partir desses computadores. Isto dissemina a destruição de dados e programas entre muitos usuários de computador. Tecnicamente, um *vírus* não rodará sem assistência, mas deverá ser inserido em outro programa, enquanto um *verme* é um programa distinto que pode rodar sem assistência.

Totais de Controle

Acúmulo de totais de dados em múltiplos pontos em um sistema de informação para garantir o processamento correto de informações.

Controles para a Computação pelo Usuário Final

Os usuários finais gerenciais são responsáveis pelos controles dos sistemas de informação em suas unidades de negócios.

Recuperação de Desastres

Métodos para garantir que uma organização se recupera de desastres naturais e causados pelo homem que afetam suas operações baseadas no computador.

Criptografia

Embaralhar ou converter dados, antes da transmissão, para um código secreto que dissimula o significado dos dados para destinatários não autorizados. O mesmo que codificação.

Ergonomia

A ciência e tecnologia que enfatiza a segurança, conforto e facilidade do uso de máquinas operadas por humanos tais como computadores. A meta da ergonomia é produzir sistemas que sejam amigáveis ao usuário, ou seja, seguros, confortáveis e fáceis de utilizar. A ergonomia também é conhecida como engenharia de fatores humanos.

Impactos Éticos e Sociais

Esses incluem (1) emprego, (2) individualidade, (3) saúde, (4) privacidade, (5) soluções sociais e (6) condições de trabalho.

Impactos Éticos e Sociais da TI – Emprego

O impacto da TI sobre o emprego é uma das principais preocupações éticas e está diretamente relacionado ao uso de computadores para a realização da automação. A TI gerou novos empregos e aumentou a produtividade, entretanto, também provocou uma redução significativa em alguns tipos de oportunidades de emprego.

Impactos Éticos e Sociais da TI – Saúde

A TI no local de trabalho levanta uma série de questões de saúde, incluindo problemas de saúde como estresse no trabalho, lesões em músculos do braço e pescoço, tensão ocular, exposição a radiação e até morte por acidentes provocados por computador.

Impactos Éticos e Sociais da TI – Individualidade

Os sistemas baseados em computador são criticados como sistemas impessoais que desumanizam e despersonalizam atividades e eliminam relações humanas presentes em sistemas manuais. As pessoas sentem uma perda de individualidade uma vez que alguns sistemas exigem a arregimentação do indivíduo e adesão estrita a procedimentos detalhados.

Impactos Éticos e Sociais da TI – Privacidade

A TI pode ser utilizada para armazenar e recuperar enormes quantidades de informação. Entretanto, ela também pode produzir um efeito negativo sobre o direito à privacidade de todo indivíduo.

Impactos Éticos e Sociais da TI – Soluções Sociais

A TI pode produzir muitos efeitos benéficos na sociedade. Ela está sendo utilizada para solucionar problemas humanos e sociais por meio de aplicações sociais tais como diagnósticos médicos, instruções assistidas por computador, planejamento de programa de governo, controle da qualidade ambiental e aplicação de leis.

Impactos Éticos e Sociais da TI – Condições de Trabalho

A TI eliminou algumas tarefas monótonas e perversas anteriormente executadas por pessoas. A TI tem atualizado a qualidade de trabalho, mas também está sendo criticada por relegar as pessoas a um papel de apoio "sem-fazer-nada".

Modelos Éticos – Filosofias Éticas

As escolhas éticas podem resultar de processos ou etapas comportamentais da tomada de decisão. Essas incluem egoísmo, lei natural, utilitarismo e respeito pelas pessoas.

Controles de Instalações

Métodos que protegem instalações físicas e seus conteúdos contra perda ou destruição.

Tolerância a Falhas

Computadores dotados de múltiplos processadores centrais, periféricos e softwares de sistemas que são capazes de continuar com operações mesmo que haja uma falha maior no hardware ou software.

Fire Wall

Um computador que protege redes de computadores contra a invasão filtrando todo o tráfego de rede e funcionando como um ponto seguro de transferência para acesso à e de outras redes.

Flaming

Flaming é a prática de enviar mensagens de e-mail extremamente críticas, detrativas e muitas vezes vulgares (*flame mail)* ou mensagens por BBSs para outros usuários na Internet ou serviços on-line.

Hacking

(1) Uso obsessivo de um computador e (2) o acesso não autorizado e uso de sistemas de computadores.

Fatores Humanos

Capacidades de hardware e software que podem afetar o conforto, segurança, facilidade de uso e personalização pelo usuário de sistemas de informação baseados em computador.

Controles de Sistemas de Informação

Métodos e dispositivos que procuram garantir a precisão, validade e propriedade das atividades dos sistemas de informação. Os controles de sistemas de informação monitoram e mantêm a qualidade e segurança das atividades de entrada, processamento, saída e armazenamento de todo sistema de informação.

Segurança de Sistemas de Informação

Controles que garantem a precisão, integridade e segurança das atividades e recursos dos sistemas de informação. Os controles podem minimizar erros, fraude e destruição.

Segurança de Redes

A segurança de uma rede pode ser fornecida por pacotes especializados de software de sistemas conhecidos como monitores de segurança de sistemas. Esses monitores são programas que monitoram o uso dos sistemas de informação e de redes e os protegem contra o uso não autorizado, fraude e destruição.

Senhas

Uma senha é utilizada como um método de segurança que possibilita aos sistemas de computador identificarem usuários qualificados e determinarem que tipos de informações eles estão autorizados a receber.

Leis de Privacidade

Leis que regulamentam a coleção, acesso e uso de dados pessoais.

Controles de Procedimentos

Métodos que especificam como a organização dos serviços de informação deveria ser realizada para se obter segurança máxima.

Usuário Final Responsável

Usuário final que age com integridade e competência no uso da TI.

Códigos de Segurança

Senhas, códigos de identificação, códigos de contas e outros códigos que limitam o acesso e uso de recursos dos sistemas de informação baseados em computador para usuários autorizados.

Pirataria de Software

Cópia não autorizada de software.

Spamming

Spamming é o envio indiscriminado de e-mail não solicitado para muitos usuários da Internet. O *spamming* é a tática favorita dos remetentes de massas de propagandas não solicitadas ou *junk e-mail*.

Monitor de Segurança de Sistemas

Software que controla o acesso e uso de um sistema de computação.

RESPOSTAS PARA SIGa em frente

1. O que pode ser feito para melhorar a segurança na Internet? Dê exemplos de hardware, software, rede e outros controles e medidas de segurança.

As respostas dos alunos irão variar. Entretanto, algumas questões podem ser mais policiamento, protocolos padrão, criptografia, acesso seguro à rede, etc.

2. Que problemas potenciais de segurança você vê no uso crescente de intranets e extranets nos negócios? O que poderia ser feito para resolver esses problemas? Cite alguns exemplos.

As respostas dos alunos irão variar. Entretanto, com o crescente uso empresarial de intranets e extranets, não há dúvida de que o número de problemas potenciais de segurança também aumenta. Questões como hacking, alteração de dados, acesso não autorizado a dados, etc. se tornarão problemas fundamentais de segurança.

Para solucionar esses problemas, as empresas devem continuar a tomar precauções em áreas como criptografia, fire walls, sites seguros da Internet, etc.

3. Que técnicas de inteligência artificial as empresas podem adotar para melhorar a segurança dos computadores e combater o crime com o uso do computador?

Fazer com que os sistemas utilizem controles biométricos, tais como sistemas de reconhecimento de voz, para identificação de pessoas autorizadas. Sistemas de criptografia de dados para transmissão segura de dados.

4. Quais os controles necessários para melhorar a segurança na computação pelo usuário final? Cite um exemplo de três controles que poderiam ser utilizados em sua faculdade ou trabalho.

- *Métodos de teste de sistemas desenvolvidos pelo usuário para submissão às políticas e procedimentos de trabalho da empresa.*
- *Métodos de notificação de outros usuários quando há o planejamento de mudanças em sistemas desenvolvidos pelo usuário para encargos cruciais.*
- *Controle por meio da documentação dos sistemas desenvolvidos pelo usuário.*
- *Treinamento de diversas pessoas quanto à operação e manutenção de um sistema.*
- *Um processo formal para avaliação e aquisição de novo hardware e software.*
- *Procedimentos formais para backup e recuperação para todos os sistemas de usuários.*
- *Controles de segurança ao acesso para sistemas de computador de usuários e empresas, redes e bancos de dados.*

5. O que é recuperação de desastres? Como ela poderia ser implementada em sua faculdade ou trabalho?

Recuperação de desastres são métodos para garantir que uma organização se recupere de desastres naturais e provocados pelo homem que afetam suas operações baseadas no computador.

As respostas dos alunos irão variar. Entretanto, deve-se desenvolver um plano de recuperação de desastres que especifique quais funcionários participarão na recuperação do desastre, quais serão suas obrigações. que hardware, software e instalações serão utilizados e a prioridade de aplicações que serão processadas. Acordos com outras empresas para o uso de instalações alternativas como local de recuperação de desastres e armazenamento externo dos bancos de dados de uma organização também fazem parte de um esforço eficaz de recuperação de desastres.

6. Consulte o Caso Concreto sobre a BuyDirect e Outras Empresas neste capítulo. Como os encarregados da aplicação das leis poderiam ajudar a combater a fraude em cartões de crédito no comércio eletrônico?

Primeiramente, os oficiais encarregados da aplicação das leis devem reconhecer que a fraude em cartões de crédito no comércio eletrônico é crime. Roubo é roubo – não importa se foi cometido por meio do uso da tecnologia ou violência. Os oficiais encarregados da aplicação das leis precisam ser educados para ajudarem a combater esta crescente área do crime.

7. Existe hoje uma crise ética nos negócios? Qual papel a tecnologia da informação desempenha nas práticas de negócios antiéticas?

A TI tornou mais fácil se comunicar, trabalhar de maneira cooperativa, compartilhar recursos e tomar decisões, tudo eletronicamente. Entretanto, a TI também tornou possível engajar-se eletronicamente em práticas éticas bem como antiéticas em qualquer parte do mundo.

8. Que decisões empresariais você tomará como gerente que terão uma dimensão ética e uma dimensão de TI? Cite vários exemplos para ilustrar sua resposta.

Exemplos são decisões para implementar a TI que executem a privacidade dos funcionários, a segurança dos registros da empresa e a segurança do local de trabalho.

9. Consulte o Caso Concreto sobre a Warroom Research e o Sun-Trust Banks neste capítulo. Você acha que os PCs e redes que você utiliza estão devidamente protegidos? Por quê?

As respostas dos alunos irão variar. Sem dúvida, se eles não se sentem confortáveis com o nível de proteção de seu ambiente, eles devem discutir a questão com os indivíduos responsáveis.

10. Quais seriam exemplos de um efeito positivo e de um efeito negativo do uso da tecnologia da informação para cada uma das dimensões éticas e sociais ilustradas na Figura 12.13? Explique algumas de suas respostas.

Emprego: A TI gerou muitos novos empregos e aumento da produtividade. A TI provocou uma redução significativa em alguns tipos de oportunidades de emprego.

Individualidade: Os sistemas computadorizados podem ser ergonomicamente projetados para acomodar fatores humanos. Eles eliminam as relações humanas presentes em sistemas manuais.

Condições de Trabalho: A TI eliminou algumas tarefas monótonas e perversas no escritório e na fábrica que anteriormente tinham de ser executadas pelas pessoas. Muitas operações automatizadas relegam as pessoas a um papel de apoio "sem-fazer-nada".

Privacidade: A identificação por chamada pode permitir que os usuários identifiquem ligações de vendedores ou ligações de brincadeira. A TI permite que os supervisores monitorem conversas e registros particulares dos funcionários.

Crime com o uso do computador: A TI pode ser utilizada na aplicação das leis. A TI pode ser utilizada como uma ferramenta na prática de crimes.

Questões de Saúde: A TI pode ser utilizada em diagnósticos médicos. O uso intenso de computadores pode causar problemas de saúde como estresse no trabalho, lesão nos músculos do braço e pescoço, tensão ocular e exposição à radiação.

Soluções Sociais: A TI pode ser utilizada para solucionar problemas humanos e sociais por meio de aplicações sociais como diagnósticos médicos, instruções assistidas por computador, planejamento de programas de governo, controle da qualidade ambiental e aplicação das leis. Os sistemas de informação baseados no computador podem violar leis e regulamentos anti-truste e internacionais.

RESPOSTAS PARA EM REDE

1. <u>Wal-Mart versus Amazon.com: Questões Éticas na Competição do Comércio Eletrônico</u>

a) Você acha que a contratação de funcionários de SI do Wal-Mart pelo Amazon é uma prática ética nos negócios e na TI? Por quê?
As respostas dos alunos irão variar. O que fez o Amazon não é contra a lei em termos legais. Sem dúvida, alguns alunos acharão que foi antiético. Outros acharão que existe um campo justo de ação para todos os participantes e que esses indivíduos têm o direito de mudar de um emprego para outro.

b) Como a disputa entre o Wal-Mart e o Amazon.com deve ser resolvida? Explique seu raciocínio.
As respostas dos alunos irão variar. A disputa entre o Wal-Mart e o Amazon.com é muito complexa. Questões como conhecimento e know-how dos funcionários internos de uma empresa são bastante conservadas e protegidas dentro de empresas maiores. Entretanto, as organizações continuarão a experimentar a pressão de outras empresas no que diz respeito a roubar seus principais funcionários.

2. <u>O Happy99, o Melissa e a Kelly Services: Vírus por E-mail e Software Antivírus</u>

a) Qual o prejuízo causado aos usuários e redes empresariais por vírus de e-mail como o Happy99.exe e o Melissa?
Os prejuízos causados aos usuários e redes empresariais por vírus de e-mail como o Happy99.exe e o Melissa podem ser extremamente sérios. O vírus Happy99.exe não tenta destruir arquivos em máquinas infectadas, mas ele envia mensagens por e-mail e grupos de notícias sem o conhecimento da vítima e pode causar redução na velocidade da rede ou até destruir servidores de e-mails empresariais. O vírus Melissa é considerado mais perigoso que o Happy99. Este vírus pode copiar a si mesmo nos 50 endereços de e-mail do arquivo de e-mail pessoal da estação de trabalho do usuário e pode fazer com que documentos sejam enviados por e-mail para outras pessoas sem aviso. Com este vírus, há uma falha potencial de segurança tanto para empresas como para governos.

b) Como uma empresa e seus usuários devem proteger seus PCs e redes dos vírus de computador?

As empresas e usuários podem proteger seus PCs e redes dos vírus de computador estabelecendo políticas e procedimentos. Eles podem fornecer a garantia de que os usuários estão protegidos de ameaças de vírus instalando software antivírus como o software de proteção contra vírus McAfee e Norton. Além disso, os administradores de sistemas e especialistas em SI podem monitorar e proteger seus sites utilizando métodos como os que foram discutidos pela Kelly Services no problema.

3. Rita Berzin e o Excite: Vantagens e desvantagensrelacionadas com a Privacidade no Comércio Eletrônico

a) É uma prática ética nos negócios ou na TI as empresas na Web coletarem informações sobre você e suas atividades na rede? Por quê?

As respostas dos alunos irão variar. Rita Berzin pode ser considerada uma vítima inocente da descoberta da Internet. Ela prontamente entrou na rede on-line para fazer compras e ter uma experiência de aprendizado. O que ela não se prontificou a fazer foi autorizar que cada um de seus movimentos fosse divulgado – o mesmo se aplica a uma pessoa que estava acompanhando seus passos de perto. Atualmente, não existem leis que considerariam o que aconteceu a Rita um crime. Se Rita soubesse que isto estava acontecendo, talvez ela não teria se disposto a participar. Rita tem o direito de esperar que sua privacidade seja protegida. Exige-se que as empresas exerçam práticas empresariais éticas.

b) O que as empresas e indivíduos devem fazer para resolver esta questão de privacidade?

Os indivíduos têm a incumbência de se conscientizarem mais sobre como sua atividade está sendo monitorada, registrada e utilizada por outros. As empresas devem ser forçadas a reconhecer o fato de que exige-se que elas utilizem informações particulares e confidenciais da maneira mais ética e legal possível.

RESPOSTAS PARA CONECTANDO-SE

1. A Ética do Computador: Abusos no Acesso à Internet no Local de Trabalho

a) Como alguns funcionários estão abusando do acesso on-line fornecido por suas empresas?

Os funcionários estão abusando do acesso on-line à Internet fornecido por suas empresas de várias maneiras. Eles podem usá-lo, por exemplo, para negócios pessoais, controlar atividades ilegais, roubo de serviços, flaming, etc.

b) O que as empresas devem fazer para restringir tais abusos de seus recursos de computação?

As empresas podem começar ensinando os funcionários sobre políticas e padrões estabelecidos que tenham sido desenvolvidos, tratando do modo como os recursos de computação da empresa podem ser utilizados. Em seguida, os funcionários são avisados com antecedência sobre o que a empresa considerou aceitável e quais ações merecerão ação corretiva.

Além de educação adequada, as empresas podem utilizar softwares que monitorem seu uso de recursos de computação. Eles podem bloquear funcionários, horas do dia, sites na Web, proibir o carregamento de certos tipos de arquivos, etc.

c) Você concorda com Neal Friedman em que "os funcionários... não têm direito algum à privacidade e direito algum de livre discurso utilizando recursos das empresas"? Por quê?

As respostas dos alunos irão variar.

2. Seus Direitos à Internet no Trabalho: Três Cenários Éticos

a) Você concorda com o conselho do advogado Mark Grossman em cada um dos cenários? Por quê?

b) Qual seria o seu conselho? Explique suas opiniões.

c) Identifique as filosofias éticas, valores ou modelos que você pode utilizar ao explicar sua opinião sobre cada um dos cenários.

As respostas dos alunos irão variar.

RESPOSTAS PARA ERA VIRTUAL – FATO REAL

A BuyDirect e Outras Empresas: Fraude com Cartões de Crédito no Comércio Eletrônico

1. Como acontece a fraude com cartões de crédito na Internet?

A fraude com cartões de crédito pode facilmente acontecer na Internet. Primeiro, é fácil conseguir cartões de crédito roubados e, na verdade, você pode utilizar a Internet para obtê-los.

2. Que passos uma empresa deve dar para se proteger da fraude com cartões de crédito no comércio eletrônico?

Como se afirmou no caso, algumas empresas decidiram não oferecer seus itens mais caros pela Internet. Outras preferiram não realizar o comércio eletrônico em países onde a taxa de fraude em cartões de crédito é alta. Algumas preferiram terceirizar a verificação de cartões de crédito para empresas dotadas de sofisticados (e caros) softwares antifraude baseados em redes neurais. Outras preferiram desenvolver seus próprios sistemas antifraude. Outra abordagem é adotar procedimentos de checagem off-line e verificar manualmente os cartões. Outras defesas envolvem práticas de seleção baseadas nas vendas mais típicas dos varejistas on-line.

Uma combinação de duas estratégias de defesa pode ser a melhor maneira de proteção: controle especializado da autorização e conhecimento especializado da base de clientes de sua empresa.

3. Visite o site de comércio eletrônico de uma empresa na Web. Que medidas estão sendo tomadas para reduzir ao mínimo a fraude em cartões de crédito em transações de comércio eletrônico?

As respostas dos alunos irão variar.

A Warroom Research e o Sun-Trust Banks: Defesa Contra os Ciberataques às redes

1. Qual o valor dos testes de penetração de redes para uma empresa?

O valor dos testes de penetração de redes para uma empresa é impedir que visitantes inoportunos ataquem e ganhem acesso a seus dados. As organizações consideram a segurança das informações como uma questão muito séria. Elas estão constantemente à procura de brechas na segurança em seus sistemas automatizados e desejam acabar com essas brechas antes de serem exploradas por cibercriminosos.

2. O que os hackers esperam conseguir com ataques às redes das empresas?

Os hackers esperam ganhar acesso a informações empresariais valiosas com seus ataques às redes das empresas. Eles têm o potencial de utilizar as informações que obtêm de uma maneira que poderia prejudicar seriamente a organização que sofreu o seu ataque.

3. Como as organizações devem proteger-se de ataques às redes pela nova geração de scanners de ataque?

Como se afirmou no caso, as empresas devem estabelecer procedimentos automáticos de monitoração e auditoria, além de resposta rápida de administração de sistemas. As organizações devem executar testes automáticos de vulnerabilidade várias vezes por ano. As empresas podem também utilizar equipes de especialistas em diferentes disciplinas para que descubram brechas de segurança e as fechem rapidamente.